ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 104 (2004) 263–278

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

An alternate proof of Cohn's four squares theorem

Jesse Ira Deutsch

Mathematics Department, University of Botswana, Private Bag 0022, Gaborone, Botswana

Received 2 July 2002; revised 23 May 2003

Communicated by D. Goss

Abstract

While various techniques have been used to demonstrate the classical four squares theorem for the rational integers, the method of modular forms of two variables has been the standard way of dealing with sums of squares problems for integers in quadratic fields. The case of representations by sums of four squares in $\mathbb{Q}(\sqrt{5})$ was resolved by Götzky, while those of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ were resolved by Cohn. These efforts utilized modular forms. In previous work, the author was able to demonstrate Götzky's theorem by means of the geometry of numbers. Here Cohn's theorem on representation by the sum of four squares for $\mathbb{Q}(\sqrt{2})$ is proven by a combination of geometry of numbers and quaternionic techniques.

MSC: primary 11D09; 11D57; 11P05; secondary 11Y99

Keywords: Sums of squares; Quaternions; Geometry of numbers

1. Introduction

In papers in the early 1960's, H. Cohn found analogues of sums of squares theorems for certain quadratic number fields. These papers extended the work of Götzky in the 1920s demonstrating that every totally positive integer in $\mathbb{Q}(\sqrt{5})$ is the sum of four squares of integers from that field. In particular, Cohn showed that every totally positive integer with even coefficient on the radical term in $\mathbb{Q}(\sqrt{2})$ and

E-mail address: deutschj@mopipi.ub.bw.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2003.08.005

$\mathbb{Q}(\sqrt{3})$ is the sum of four integer squares from their respective fields. The above work of Götzky and Cohn was based on the theory of modular forms of two variables, and gave the number of representations in addition to an existence proof (see [2–4,6]). Here Cohn's Theorem on the existence of sum of four squares representations is proven in the case of $\mathbb{Q}(\sqrt{2})$ without recourse to the theory of modular forms.

Other techniques have been used to prove the classical four squares theorem that every positive rational integer is the sum of four rational integer squares. Lagrange used infinite descent, Grace worked with the geometry of numbers, and Hurwitz utilized a special ring of quaternions (see [8,9]). In a previous paper, the author gave an alternate proof of Götzky's result for $\mathbb{Q}(\sqrt{5})$ by means of geometry of numbers. Using a convex figure in $\mathbb{R}^8$ called a spherical diamond, it was possible by means of geometry of numbers to demonstrate that for each algebraic integer prime ρ in $\mathbb{Q}(\sqrt{5})$ there exist algebraic integers $\alpha,\ \beta,\ \gamma,\ \delta$ and κ such that

$$\alpha^2+\beta^2+\gamma^2+\delta^2=\kappa\rho, \tag{1.1}$$

where $|\kappa\kappa^*|\leqslant 8$. Here * means conjugation with respect to $\mathbb{Q}(\sqrt{5})$. From this point, some number theory in the ring of integers of $\mathbb{Q}(\sqrt{5})$ eliminated all cases except that of κ a unit. The four square theorem then follows (see [5]). Due to larger bounds and differences in number theory of the corresponding ring, the above approach is insufficient by itself for the case of sums of four squares in $\mathbb{Q}(\sqrt{2})$.

Hurwitz's approach to the classical four squares theorem used the norm Euclidean property of the ring $\mathbb{Z}\left[1,\ \mathbf{i},\ \mathbf{j},\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\right]$. However, one key step in the proof required the use of the result in elementary number theory that for every rational prime p there exists rational integers a and b such that $a^2+b^2+1=kp$ with $k<p$. While it is not clear if there is an analogue to this result in quadratic fields, this difficulty can be avoided by using the conclusions available from the geometry of numbers.

In contrast to Hurwitz's quaternions, we use the ring of *cubian* quaternions. Letting $O(\sqrt{2})$ represent the ring of algebraic integers in $\mathbb{Q}(\sqrt{2})$, the cubians are the $O(\sqrt{2})$-module with generators $\{1,\ \sqrt{2}(1+\mathbf{i})/2,\ \sqrt{2}(1+\mathbf{j})/2, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\}$. This set is a ring and a principal ideal domain (see [1,11]). Recall than an associate of an element of a ring is the product of that element with a unit of the ring on the left or right. While each Hurwitz quaternion has an associate with integer coefficients in the standard quaternion basis $\{1,\mathbf{i},\mathbf{j},\mathbf{k}\}$, it is not the case that every cubian has an associate with $O(\sqrt{2})$ coefficients in that basis. However, some weaker results are proven that combined with knowledge of factorization into primes of $O(\sqrt{2})$ suffice to obtain Cohn's result for $\mathbb{Q}(\sqrt{2})$. For information on the classical case see Hardy and Wright [8, Chapter XX] and Herstein [9].

To fix notation, let $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ be the standard quaternions whose squares are -1 and whose products are anti-commutative, i.e. $\mathbf{ij}=-\mathbf{ji}$, etc. We use $\mathbb{H}$ to represent the ring of all real quaternions, that is, all real linear combinations of the elements 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. Bold type is used to represent a quaternion variable, so that a typical element

of $\mathbb{H}$ is of the form $\mathbf{q} = q_1 + q_2\mathbf{i} + q_3\mathbf{j} + q_4\mathbf{k}$ with $q_1, \ldots, q_4$ real numbers. Quaternion conjugation is denoted by placing a bar above the variable. Thus $\bar{\mathbf{q}}$ is the same as $\mathbf{q}$ except for sign changes in the coefficients of $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$. N represents the quaternion norm, so that $N(\mathbf{q}) = \mathbf{q} \cdot \bar{\mathbf{q}} = q_1^2 + \cdots + q_4^2$.

For R a subring of the real numbers, and $\mathbf{s}_1, \ldots, \mathbf{s}_k$ real quaternions, we define $R[\mathbf{s}_1, \ldots, \mathbf{s}_k]$ as the R module generated by $\mathbf{s}_1, \ldots \mathbf{s}_k$. When R is a subring of a quadratic field, we use a star * to show conjugation with respect to the field. Thus the cubians are $\mathbb{K} = O(\sqrt{2})[1, \sqrt{2}(1+\mathbf{i})/2, \sqrt{2}(1+\mathbf{j})/2, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})]$. We define

$$\mathbf{w}_1 = 1, \quad \mathbf{w}_2 = \sqrt{2}(1+\mathbf{i})/2, \quad \mathbf{w}_3 = \sqrt{2}(1+\mathbf{j})/2, \quad \mathbf{w}_4 = \tfrac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k}). \tag{1.2}$$

2. Results from the geometry of numbers

A key result in the alternate proof of Götzky's theorem was that for every prime ρ in the algebraic integers $O(\sqrt{5})$ of $\mathbb{Q}(\sqrt{5})$ there exist κ, α, β, γ and δ in $O(\sqrt{5})$ for which $\kappa\rho = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ with κ a unit. This can be generalized using the same geometry of numbers technique employed in Deutsch [5], though the restriction on κ must be loosened.

Lemma 1. *Let p be a rational prime which splits in the ring of algebraic integers O of a real quadratic field of discriminant d. Let ρ be a prime of O dividing p. Then there exist κ, α, β, γ and δ in O such that $\kappa\rho = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ and $|\kappa\kappa^*| \leqslant 1.70 \cdot d$.*

Proof. We closely follow the proof in Deutsch [5]. Since p splits, $|\rho\rho^*| = p$. Choose rational integers a and b such that $a^2 + b^2 + 1 \equiv 0 (\mathrm{mod}\, p)$. Hence $a^2 + b^2 + 1 \equiv 0 (\mathrm{mod}\, \rho)$. Choose ε so that 1 and ε are $\mathbb{Z}$ module generators of O, i.e. $O = \mathbb{Z}[1, \varepsilon]$.

To employ the geometry of numbers approach, we need to choose a lattice and a centrally symmetric convex subset in $\mathbb{R}^8$. For the lattice we choose the set

$$(\alpha, \alpha^*, \beta, \beta^*, a\alpha + b\beta + \mu\rho, a\alpha^* + b\beta^* + \mu^*\rho^*, b\alpha - a\beta + \nu\rho, b\alpha^* - a\beta^* + \nu^*\rho^*), \tag{2.1}$$

where α, β, μ and ν run through all of O. It can be seen that this lattice is generated by the following basis elements:

$$\left\{ \begin{array}{l} (1,1,0,0,a,a,b,b), (\varepsilon,\varepsilon^*,0,0,a\varepsilon,a\varepsilon^*,b\varepsilon,b\varepsilon^*), \\ (0,0,1,1,b,b,-a,-a), (0,0,\varepsilon,\varepsilon^*,b\varepsilon,b\varepsilon^*,-a\varepsilon,-a\varepsilon^*), \\ (0,0,0,0,\rho,\rho^*,0,0), (0,0,0,0,\varepsilon\rho,\varepsilon^*\rho^*,0,0), \\ (0,0,0,0,0,0,\rho,\rho^*), (0,0,0,0,0,0,\varepsilon\rho,\varepsilon^*\rho^*) \end{array} \right\}. \tag{2.2}$$

The size of the lattice is the absolute value of the determinant of a basis, which is $|(\varepsilon - \varepsilon^*)^4 \rho^2 (\rho^*)^2|$ or d^2p^2. We apply Minkowski's convex body theorem to the

spherical diamond $\mathscr{C}(r)$ in $\mathbb{R}^8$ defined by

$$\sqrt{x_1^2+x_2^2+x_3^2+x_4^2}+\sqrt{x_5^2+x_6^2+x_7^2+x_8^2}\leqslant r. \tag{2.3}$$

Using Deutsch [5, Lemma 8] we choose r such that

$$\frac{\pi^4}{280}r^8\geqslant 2^8\cdot d^2\cdot p^2 \quad\Leftrightarrow\quad r^8\geqslant\frac{2^8\cdot d^2\cdot 280}{\pi^4}p^2 \tag{2.4}$$

so $r=2.2822d^{1/4}p^{1/4}$ suffices. Minkowski's geometry of numbers gives us algebraic integers, not all zero, such that

$$\alpha^2+\beta^2+\gamma^2+\delta^2=\kappa\rho \tag{2.5}$$

and

$$\sqrt{\kappa\rho}+\sqrt{\kappa^*\rho^*}\leqslant 2.2822d^{1/4}p^{1/4} \tag{2.6}$$

so

$$\begin{aligned}&2\sqrt{\sqrt{\kappa\rho\kappa^*\rho^*}}\leqslant\sqrt{\kappa\rho}+\sqrt{\kappa^*\rho^*}\leqslant 2.2822d^{1/4}p^{1/4}\\ &|\kappa\rho\kappa^*\rho^*|^{1/4}\leqslant(2.2822/2)d^{1/4}p^{1/4}\\ &|\kappa\kappa^*|\leqslant 1.6955d.\end{aligned} \tag{2.7}$$

That proves the Lemma. □

Specializing to the case of $\mathbb{Q}(\sqrt{2})$ we can get a tighter bound.

Lemma 2. *Let ρ be a prime in $O(\sqrt{2})$. Then there exist κ, α, β, γ and δ in $O(\sqrt{2})$ such that $\kappa\rho=\alpha^2+\beta^2+\gamma^2+\delta^2$ and $|\kappa\kappa^*|\leqslant 9$.*

Proof. Let ρ lie above the rational prime p. There are three cases.

If p is inert then ρ is an associate of p. The classical four squares theorem for rational integers shows that we can choose κ as a unit of $O(\sqrt{2})$.

If p ramifies then $p=2$ and ρ must be an associate of $\sqrt{2}$. Noting the trivial equation $\sqrt{2}\sqrt{2}=1^2+1^2$ we may choose κ as an associate of $\sqrt{2}$. Thus $|\kappa\kappa^*|=2$ which suffices for the Lemma.

Suppose that p splits. Note the discriminant of $O(\sqrt{2})$ is 8. By Lemma 1 there exists $\kappa\in O(\sqrt{2})$ such that $\kappa\rho$ is the sum of four squares and $|\kappa\kappa^*|\leqslant 1.7d=13.56$. Hence $|\kappa\kappa^*|\leqslant 13$.

Let q be a rational prime that is inert in $O(\sqrt{2})$ and which divides $\kappa\kappa^*$. Being prime implies q divides κ or κ^*. But if q divides one, it must also divide the other. Hence q^2

divides $\kappa\kappa^*$. Since 3, 5, 11 and 13 are inert in $O(\sqrt{2})$ we observe that $|\kappa\kappa^*|$ cannot equal any of $\{3,5,6,10,11,12,13\}$. Hence $|\kappa\kappa^*| \leqslant 9$. □

3. The cubians

It has already been noted that the cubians $\mathbb{K}$ form a ring and are a principal ideal domain for each of the left ideals and the right ideals. There are 48 units of norm one in $\mathbb{K}$ of which only a subset will be needed for our purposes. For details see Vignéras [11].

Lemma 3. *The following are units in* $\mathbb{K}$ *of norm* 1.

$$\pm\left\{\begin{array}{l}\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4, \sqrt{2}\mathbf{w}_2 - \mathbf{w}_1, \sqrt{2}\mathbf{w}_4 - \mathbf{w}_3, \sqrt{2}\mathbf{w}_3 - \mathbf{w}_1,\\ -\mathbf{w}_4 + \sqrt{2}\mathbf{w}_3 + \sqrt{2}\mathbf{w}_2 - \mathbf{w}_1, \mathbf{w}_3 + \mathbf{w}_2 - \sqrt{2}\mathbf{w}_1, \sqrt{2}\mathbf{w}_4 - \mathbf{w}_2,\\ \mathbf{w}_4 - \mathbf{w}_1, \mathbf{w}_2 - \sqrt{2}\mathbf{w}_1, \mathbf{w}_4 - \sqrt{2}\mathbf{w}_3, \mathbf{w}_3 - \sqrt{2}\mathbf{w}_1,\\ -\sqrt{2}\mathbf{w}_4 + 2\mathbf{w}_3 + \mathbf{w}_2 - \sqrt{2}\mathbf{w}_1, \mathbf{w}_4 - \sqrt{2}\mathbf{w}_3 + \mathbf{w}_1,\\ -\mathbf{w}_4 + \sqrt{2}\mathbf{w}_3 + \sqrt{2}\mathbf{w}_2 - 2\mathbf{w}_1, \sqrt{2}\mathbf{w}_4 - \mathbf{w}_3 - \mathbf{w}_2 + \sqrt{2}\mathbf{w}_1,\\ \sqrt{2}\mathbf{w}_4 - \mathbf{w}_3 - \mathbf{w}_2\end{array}\right\}. \tag{3.1}$$

Proof. First note that $\mathbb{K}$ is closed under conjugation since $\bar{\mathbf{w}}_1 = \mathbf{w}_1$, $\bar{\mathbf{w}}_2 = \sqrt{2}\mathbf{w}_1 - \mathbf{w}_2$, $\bar{\mathbf{w}}_3 = \sqrt{2}\mathbf{w}_1 - \mathbf{w}_3$, $\bar{\mathbf{w}}_4 = \mathbf{w}_1 - \mathbf{w}_4$. The quaternions listed above all have norm 1 as is easily demonstrated by computer algebra. The inverse of any quaternion of norm 1 is its conjugate. For the quaternions above this means the inverse is an element of $\mathbb{K}$. Hence the quaternions in (3.1) are units of $\mathbb{K}$.

These units were derived by multiplying $\mathbf{w}_1$ through $\mathbf{w}_4$ together numerous times and in various combinations. □

Lemma 4. $\mathbb{K} \cap \mathbb{R} = O(\sqrt{2})$.

Proof. As $1 \in \mathbb{K}$ it is clear that $O(\sqrt{2}) \subseteq \mathbb{K} \cap \mathbb{R}$. In the other direction, write a typical $\mathbf{a} \in \mathbb{K}$ as $\mathbf{a} = \alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2 + \alpha_3\mathbf{w}_3 + \alpha_4\mathbf{w}_4$ where $\alpha_1, \ldots, \alpha_4 \in O(\sqrt{2})$. Suppose that $\mathbf{a} \in \mathbb{R}$. Then, as the $\mathbf{k}$ coefficient of $\mathbf{a}$ is zero we must have $\alpha_4 = 0$. Considering the $\mathbf{j}$ coefficient we find $\alpha_3 = 0$. Similarly for the $\mathbf{i}$ coefficient, implying $\alpha_2 = 0$. Thus $\mathbf{a} = \alpha_1\mathbf{w}_1 \in \mathbb{R}$. Therefore, $\mathbb{K} \cap \mathbb{R} \subseteq O(\sqrt{2})$ and the Lemma follows. □

Lemma 5. *For all* $\mathbf{a} \in \mathbb{K}$ *the quaternionic norm* $N(\mathbf{a}) \in O(\sqrt{2})$.

Proof. $N(\mathbf{a}) = \mathbf{a}\bar{\mathbf{a}}$ is an element of the ring $\mathbb{K}$ as this ring is closed under conjugation. By the previous Lemma, $N(\mathbf{a}) \in O(\sqrt{2})$. □

Hurwitz's proof of the rational four squares theorem depends upon the fact that every quaternion in his special ring has an associate in $\mathbb{Z}[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. In contrast, numerical computation tends to imply that even if we permit multiplication by units on both sides of an element of $\mathbb{K}$ we do not always get at least one such two sided associate into $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. However, the following weaker results suffice for our purposes.

Lemma 6. *For all* $\mathbf{q}\in\mathbb{K}$ *there exists a quaternion unit* $\mathbf{u}\in\mathbb{K}$ *of norm* 1 *such that* $\sqrt{2}\mathbf{qu}$ *has* $O(\sqrt{2})$*–integer coefficients, i.e.* $\sqrt{2}\,\mathbf{qu}\in O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$.

Proof. Let $\mathbf{q}=\alpha_1\mathbf{w}_1+\alpha_2\mathbf{w}_2+\alpha_3\mathbf{w}_3+\alpha_4\mathbf{w}_4$, where $\alpha_1,\ldots,\alpha_4\in O(\sqrt{2})$. Write

$$\mathbf{q}=2(\gamma_1\mathbf{w}_1+\gamma_2\mathbf{w}_2+\gamma_3\mathbf{w}_3+\gamma_4\mathbf{w}_4)+(\delta_1\mathbf{w}_1+\delta_2\mathbf{w}_2+\delta_3\mathbf{w}_3+\delta_4\mathbf{w}_4), \tag{3.2}$$

where $\gamma_1,\ldots,\gamma_4\in O(\sqrt{2})$ and $\delta_1,\ldots,\delta_4\in O(\sqrt{2})/(2)$. Note that a full set of residues of $O(\sqrt{2})$ modulo 2 can be chosen as $\{0,1,\sqrt{2},1+\sqrt{2}\}$. Computation shows that for all possible values of $\delta_1,\ldots,\delta_4$ there exists a quaternion unit $\mathbf{u}$ in (3.1) such that $\sqrt{2}(\delta_1\mathbf{w}_1+\cdots+\delta_4\mathbf{w}_4)\mathbf{u}$ is an element of $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. See Table 1 for examples of the relevant computations. Also

$$\sqrt{2}\cdot 2\cdot\left(\sum_{t=1}^{4}\gamma_t\mathbf{w}_t\right)\cdot\mathbf{u}=2\cdot\sqrt{2}\cdot\sum_{t=1}^{4}\hat{\gamma}_t\mathbf{w}_t \tag{3.3}$$

with $\hat{\gamma}_1,\ldots,\hat{\gamma}_4\in O(\sqrt{2})$ as $\mathbb{K}$ is closed under quaternion multiplication. However, two times any element of $\mathbb{K}$ must be in $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$ as the denominators of the

Table 1
Some associates of elements of $\mathbb{K}$ whose dilations by $\sqrt{2}$ are in $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$

Quaternion $\mathbf{q}$	Unit $\mathbf{u}$	$\sqrt{2}\mathbf{qu}$
$\vdots$	$\vdots$	$\vdots$
$\sqrt{2}\mathbf{w}_1$	$\mathbf{w}_1$	2
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_4$	$\mathbf{w}_2$	$\sqrt{2}+(\sqrt{2}+1)\mathbf{i}+\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+\sqrt{2}\mathbf{w}_4$	$\mathbf{w}_1$	$3+\mathbf{i}+\mathbf{j}+\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+(\sqrt{2}+1)\mathbf{w}_4$	$\mathbf{w}_2$	$\sqrt{2}+(2\sqrt{2}+1)\mathbf{i}+(\sqrt{2}+1)\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3$	$\mathbf{w}_1$	$3+\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3+\mathbf{w}_4$	$\mathbf{w}_3$	$\sqrt{2}+(2\sqrt{2}+1)\mathbf{j}+\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3+\sqrt{2}\mathbf{w}_4$	$\mathbf{w}_1$	$4+\mathbf{i}+2\mathbf{j}+\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3+(\sqrt{2}+1)\mathbf{w}_4$	$\mathbf{w}_3$	$\sqrt{2}+(3\sqrt{2}+1)\mathbf{j}+(\sqrt{2}+1)\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+\sqrt{2}\mathbf{w}_3$	$\mathbf{w}_1$	$(\sqrt{2}+2)+\sqrt{2}\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+\sqrt{2}\mathbf{w}_3+\mathbf{w}_4$	$\mathbf{w}_2$	$(\sqrt{2}+1)+(\sqrt{2}+2)\mathbf{i}+2\mathbf{j}-\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+\sqrt{2}\mathbf{w}_3+\sqrt{2}\mathbf{w}_4$	$\mathbf{w}_1$	$(\sqrt{2}+3)+\mathbf{i}+(\sqrt{2}+1)\mathbf{j}+\mathbf{k}$
$\vdots$	$\vdots$	$\vdots$

generators are 1, $\sqrt{2}$ or 2. Hence

$$\sqrt{2}\mathbf{qu} = \sqrt{2}\cdot 2\cdot\left(\sum_{t=1}^{4}\gamma_t\mathbf{w}_t\right)\cdot\mathbf{u} + \sqrt{2}\cdot\left(\sum_{t=1}^{4}\delta_t\mathbf{w}_t\right)\cdot\mathbf{u} \tag{3.4}$$

is an element of $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. □

We now need a more delicate result on associates. If we consider certain primes in $O(\sqrt{2})$ such as $3+\sqrt{2}$ and $5+\sqrt{2}$ we know that these cannot be written as sums of squares. Yet the product $(3+\sqrt{2})(5+\sqrt{2}) = 17+8\sqrt{2}$ can be written as the sum of four squares. This situation is related to the following lemma.

Lemma 7. *Let* $\mathbf{q}\in\mathbb{K}$. *Thus* $N(\mathbf{q})\in O(\sqrt{2})$. *Suppose* $N(\mathbf{q}) = a+b\sqrt{2}$ *where a is an odd rational integer and b is an even rational integer. Then there exists a quaternion unit* $\mathbf{u}\in\mathbb{K}$ *of norm* 1 *such that* $\mathbf{qu}\in O(\sqrt{2})\,[1,\mathbf{i},\mathbf{j},\mathbf{k}]$.

Proof. Consider the norm of a typical element of $\mathbb{K}$.

$$N((a_1+b_1\sqrt{2})\mathbf{w}_1 + (a_2+b_2\sqrt{2})\mathbf{w}_2 + (a_3+b_3\sqrt{2})\mathbf{w}_3 + (a_4+b_4\sqrt{2})\mathbf{w}_4), \tag{3.5}$$

where $a_1,\ldots,a_4,b_1,\ldots,b_4\in\mathbb{Z}$. By Lemma 5 this expression must simplify to $A+B\sqrt{2}$ where A and B are rational integers. Computer algebra shows that A and B are polynomials in the a's and b's with rational integer coefficients. Also

$$\begin{aligned} A &\equiv a_1^2+a_2^2+a_3^2+a_4^2+a_1a_4+a_2a_3 \pmod 2,\\ B &\equiv a_1a_2+a_1a_3+a_2a_4+a_3a_4+a_4b_1\\ &\quad + a_3b_2+a_2b_3+a_1b_4 \pmod 2. \end{aligned} \tag{3.6}$$

Note that if we take rational integers $c_1,\ldots,c_4$ and $d_1,\ldots,d_4$ such that $c_t\equiv a_t \pmod 2$ and $d_t\equiv b_t \pmod 2$ for $t=1,2,3,4$ and compute the quaternion norm of $(c_1+d_1\sqrt{2})\mathbf{w}_1+\cdots+(c_4+d_4\sqrt{2})\mathbf{w}_4$ then the values of A and B modulo 2 do not change.

As in the previous Lemma let $\mathbf{q} = \alpha_1\mathbf{w}_1+\alpha_2\mathbf{w}_2+\alpha_3\mathbf{w}_3+\alpha_4\mathbf{w}_4$ where $\alpha_t\in O(\sqrt{2})$ for $t=1,\ldots,4$. Again decompose $\mathbf{q}$ as in (3.2), where $\gamma_1,\ldots,\gamma_4\in O(\sqrt{2})$ and $\delta_1,\ldots,\delta_4\in O(\sqrt{2})/(2)$. Let $\mathbf{d} = \delta_1\mathbf{w}_1+\cdots+\delta_4\mathbf{w}_4$. Then $\alpha_t\equiv\delta_t \pmod 2$ in $O(\sqrt{2})$ for $t=1,\ldots,4$. Thus the rational coefficients of α_t and δ_t are congruent modulo 2 in $\mathbb{Z}$ and the same holds for the corresponding irrational coefficients.

Consequently, the rational coefficient of $N(\mathbf{q})$ is congruent modulo 2 to the rational coefficient of $N(\mathbf{d})$, and the irrational coefficient of $N(\mathbf{q})$ is also congruent modulo 2 to the irrational coefficient of $N(\mathbf{d})$.

Computation shows that for every possible value of $\mathbf{d}$ such that the rational coefficient of $N(\mathbf{d})$ is odd, and the coefficient of $\sqrt{2}$ in $N(\mathbf{d})$ is even, there exists a quaternion unit $\mathbf{u}$ in (3.1) such that $\mathbf{du}$ is an element of $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. See Table 2

Table 2
Some restricted elements of $\mathbb{K}$ with associates in $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$

Quaternion $\mathbf{q}$	Norm	Unit $\mathbf{u}$	$\mathbf{qu}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{w}_1+\mathbf{w}_4$	3	$\mathbf{w}_4$	$\mathbf{i}+\mathbf{j}+\mathbf{k}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_3$	5	$\mathbf{w}_1$	$2+\mathbf{j}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_3+\mathbf{w}_4$	9	$\mathbf{w}_4$	$2\mathbf{i}+2\mathbf{j}+\mathbf{k}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_2$	5	$\mathbf{w}_1$	$2+\mathbf{i}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_2+\mathbf{w}_4$	9	$\mathbf{w}_4$	$2\mathbf{i}+\mathbf{j}+2\mathbf{k}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_2+\sqrt{2}\mathbf{w}_3$	11	$\mathbf{w}_1$	$3+\mathbf{i}+\mathbf{j}$
$\mathbf{w}_1+\sqrt{2}\mathbf{w}_2+\sqrt{2}\mathbf{w}_3+\mathbf{w}_4$	17	$\mathbf{w}_4$	$3\mathbf{i}+2\mathbf{j}+2\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3$	5	$\mathbf{w}_3$	$1+2\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+\mathbf{w}_3+\sqrt{2}\mathbf{w}_4$	11	$\mathbf{w}_3$	$1+3\mathbf{j}+\mathbf{k}$
$\sqrt{2}\mathbf{w}_1+(\sqrt{2}+1)\mathbf{w}_3$	$7+4\sqrt{2}$	$\mathbf{w}_3$	$1+(\sqrt{2}+2)\mathbf{j}$
$\sqrt{2}\mathbf{w}_1+(\sqrt{2}+1)\mathbf{w}_3+\sqrt{2}\mathbf{w}_4$	$13+6\sqrt{2}$	$\mathbf{w}_3$	$1+(\sqrt{2}+3)\mathbf{j}+\mathbf{k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

for examples of the corresponding computation. Thus

$$\mathbf{qu}=2\cdot\left(\sum_{t=1}^{4}\gamma_t\mathbf{w}_t\right)\cdot\mathbf{u}+\mathbf{d}\cdot\mathbf{u}=2\cdot\left(\sum_{t=1}^{4}\hat{\gamma}_t\mathbf{w}_t\right)+\mathbf{d}\cdot\mathbf{u} \tag{3.7}$$

with $\hat{\gamma}_t\in O(\sqrt{2})$ for all t as $\mathbb{K}$ is closed under quaternion multiplication. Since twice any element of $\mathbb{K}$ is in $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$ we find $\mathbf{qu}$ is also in $O(\sqrt{2})[1,\mathbf{i},\mathbf{j},\mathbf{k}]$. □

Suppose ρ is a totally positive prime of the ring $O(\sqrt{2})$ lying over the rational odd prime p. If $\rho=p$ does not split in $O(\sqrt{2})$ then it is the sum of four squares by the classical theorem of Lagrange. However, the case where p does split, i.e. $p\equiv\pm1(\mathrm{mod}\,8)$, must be taken care of by other means. We proceed to do this with the next few Lemmas.

Lemma 8. *Suppose ρ is a prime of the ring $O(\sqrt{2})$. Then there exists a unit λ of $O(\sqrt{2})$ and a quaternion $\mathbf{q}$ of $\mathbb{K}$ such that $N(\mathbf{q})=\lambda\rho$.*

Proof. Suppose ρ lies over the rational prime p. We consider three cases depending on how p factors in $O(\sqrt{2})$.

If p is inert, then ρ and p differ only by a factor of a unit of $O(\sqrt{2})$. By the classical four squares theorem we can find rational integers a, b, c and d such that $p=a^2+b^2+c^2+d^2$. Note that $1\in\mathbb{K}$, $\sqrt{2}\mathbf{w}_2-\mathbf{w}_1=\mathbf{i}\in\mathbb{K}$, $\sqrt{2}\mathbf{w}_3-\mathbf{w}_1=\mathbf{j}\in\mathbb{K}$ and

$2\mathbf{w}_4 - \mathbf{w}_1 - \mathbf{i} - \mathbf{j} = \mathbf{k} \in \mathbb{K}$. Let $\mathbf{q} = a\mathbf{w}_1 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Then $\mathbf{q} \in \mathbb{K}$, $N(\mathbf{q}) = p$ and we have already observed that p is a unit of $O(\sqrt{2})$ times ρ.

If p ramifies then $p = 2$. We note that $2 + \sqrt{2} = N(\mathbf{w}_1 + \mathbf{w}_2)$. Since ρ itself must equal $\sqrt{2}$ times a unit of $O(\sqrt{2})$, and $2 + \sqrt{2} = \sqrt{2} \cdot (1 + \sqrt{2})$ it is clear that ρ times a unit of $O(\sqrt{2})$ is the norm of $\mathbf{w}_1 + \mathbf{w}_2 \in \mathbb{K}$.

Suppose p splits. Then $p \equiv \pm 1 (\mathrm{mod}\, 8)$ and $\pm p = \rho \cdot \rho^*$ where ρ^* is the conjugate of ρ with respect to $\mathbb{Q}(\sqrt{2})$. Suppose further that $|\rho \cdot \rho^*| > 9$. Applying Lemma 2, there exists α, β, γ and δ in $O(\sqrt{2})$ such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \kappa\rho$ with $|\kappa\kappa^*| \leqslant 9$ and $\kappa \in O(\sqrt{2})$. Let $\mathbf{q} = \alpha\mathbf{w}_1 + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$. Then $\mathbf{q} \in \mathbb{K}$ and $N(\mathbf{q}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \kappa\rho$. Also $N(\rho\mathbf{i}) = \rho^2$ and $\rho\mathbf{i} \in \mathbb{K}$.

Since $\mathbb{K}$ is a principal right ideal domain, the right ideal generated by $\rho\mathbf{i}$ and $\mathbf{q}$ is also generated by a single element which we denote $\mathbf{r}$. As right $\mathbb{K}$ ideals we have $(\mathbf{r}) = (\rho\mathbf{i}, \mathbf{q})$. Thus there exists $\mathbf{s}, \mathbf{t} \in \mathbb{K}$ such that $\mathbf{r} = \mathbf{s} \cdot \rho\mathbf{i} + \mathbf{t} \cdot \mathbf{q}$. Also there exists $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{K}$ such that $\mathbf{v}_1\mathbf{r} = \rho\mathbf{i}$ and $\mathbf{v}_2\mathbf{r} = \mathbf{q}$. Thus $N(\mathbf{r})$ divides $N(\rho\mathbf{i})$ and $N(\mathbf{q})$ in the ring $O(\sqrt{2})$. This implies that $N(\mathbf{r})$ divides ρ^2 and $\kappa\rho$. Since $O(\sqrt{2})$ is a unique factorization domain and a principal ideal domain, $N(\mathbf{r})$ divides the greatest common divisor of ρ^2 and $\kappa\rho$. But $|\kappa\kappa^*| \leqslant 9 < |\rho\rho^*|$ and ρ is prime, so κ is relatively prime to ρ. Thus $N(\mathbf{r})$ divides ρ which implies that $N(\mathbf{r})$ is a unit or an associate of ρ.

Consider the equation $\mathbf{r} = \mathbf{s} \cdot \rho\mathbf{i} + \mathbf{t} \cdot \mathbf{q}$ and take quaternion conjugates to find $\bar{\mathbf{r}} = \rho\bar{\mathbf{i}} \cdot \bar{\mathbf{s}} + \bar{\mathbf{q}} \cdot \bar{\mathbf{t}}$. Multiplying together we find

$$N(\mathbf{r}) = \mathbf{r}\bar{\mathbf{r}} = \rho\hat{\mathbf{s}} + N(\mathbf{q})N(\mathbf{t}) \tag{3.8}$$

for some $\hat{\mathbf{s}} \in \mathbb{K}$. Note that $N(\mathbf{r})$, $N(\mathbf{q})$, and $N(\mathbf{t})$ are real numbers. This implies that $\hat{\mathbf{s}}$ is real, and by Lemma 4 must be an element of $O(\sqrt{2})$. Hence ρ divides $N(\mathbf{r})$ in $O(\sqrt{2})$. Together with the previous result we conclude that $N(\mathbf{r})$ must be an associate of ρ, i.e. equal to ρ times a unit.

Suppose p splits and $|\rho \cdot \rho^*| \leqslant 9$. The only case is $p = 7$. We note that $3 + \sqrt{2} = N(\mathbf{w}_2 + \sqrt{2}\mathbf{w}_3)$ and $3 - \sqrt{2} = N(\mathbf{w}_2 - \sqrt{2}\mathbf{w}_3)$. Since $7 = (3 + \sqrt{2})(3 - \sqrt{2})$ any $O(\sqrt{2})$ prime ρ of norm 7 is only a factor of a unit off from $3 + \sqrt{2}$ or $3 - \sqrt{2}$. This completes the proof. □

Lemma 9. *Let ρ be a totally positive prime of the ring $O(\sqrt{2})$ lying over the rational prime p. Suppose p is congruent to* 1 *modulo* 8. *Then ρ can be written as the sum of four squares of algebraic integers from $O(\sqrt{2})$.*

Proof. Write $\rho = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$. Since ρ is totally positive

$$\rho\rho^* = \pm p \Rightarrow \rho\rho^* = +p. \tag{3.9}$$

So $a^2 - 2b^2 = p \equiv 1 (\mathrm{mod}\, 8)$. All odd numbers squared are congruent to one modulo 8 while the squares of even numbers are congruent to zero or four. Since $a^2 - 2b^2$ is congruent to one modulo 8 we must have a odd. That implies $2b^2 \equiv 0 (\mathrm{mod}\, 8)$ which

implies $b^2 \equiv 0 (\mathrm{mod}\, 4)$ so b must be even. Thus we find that $\rho \equiv a + b\sqrt{2} \equiv 1 (\mathrm{mod}\, 2)$ in $O(\sqrt{2})$.

By the previous Lemma there exists a quaternion $\mathbf{q} \in \mathbb{K}$ and a unit $\lambda \in O(\sqrt{2})$ such that $N(\mathbf{q}) = \lambda\rho$. Considering the basis of $\mathbb{K}$ we may write $\mathbf{q} = \alpha 1 + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ where $\alpha, \beta, \gamma, \delta \in \frac{1}{2}O(\sqrt{2})$. Thus

$$\lambda\rho = N(\mathbf{q}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0. \tag{3.10}$$

Taking conjugates with respect to $O(\sqrt{2})$ we find $\lambda^*\rho^*$ is also a sum of four squares and strictly greater than zero. These last two relations imply that $\lambda\rho$ is totally positive. Since ρ is totally positive we conclude that the unit λ is totally positive. As a unit, we may write λ as $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$. From total positivity, the sign on λ must be positive, which then forces the exponent to be even, $n = 2m$. So $\lambda = (3 + 2\sqrt{2})^m$. It is now easy to see that $N(\mathbf{q})$ simplifies to 1 modulo 2 in $O(\sqrt{2})$. By Lemma 7 above, there exists a quaternion unit $\mathbf{u} \in \mathbb{K}$ of norm 1 such that $\mathbf{qu} \in O(\sqrt{2})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$. Write $\mathbf{qu} = \hat{\alpha}1 + \hat{\beta}\mathbf{i} + \hat{\gamma}\mathbf{j} + \hat{\delta}\mathbf{k}$. We find

$$(1+\sqrt{2})^{2m}\rho = N(\mathbf{q}) = N(\mathbf{qu}) = (\hat{\alpha})^2 + (\hat{\beta})^2 + (\hat{\gamma})^2 + (\hat{\delta})^2. \tag{3.11}$$

Dividing both sides by the unit square factor $(1+\sqrt{2})^{2m}$ gives a representation of ρ as the sum of four squares from $O(\sqrt{2})$. □

Lemma 10. *Let ρ, ν be totally positive primes of the ring $O(\sqrt{2})$ lying over rational primes p and q respectively. Suppose that each of p and q are congruent to -1 modulo 8. Then the product $\rho\nu$ can be written as the sum of four squares from $O(\sqrt{2})$.*

Proof. Write $\rho = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$. Since ρ is totally positive we find that $|\rho\rho^*| = p$ implies $\rho\rho^* = +p$. Thus $a^2 - 2b^2 = p \equiv -1 (\mathrm{mod}\, 8)$. For the above to hold, a must be odd. Then $a^2 \equiv 1 (\mathrm{mod}\, 8)$ yields $-2b^2 \equiv -2 (\mathrm{mod}\, 8)$. That implies $b^2 \equiv 1 (\mathrm{mod}\, 4)$ which tells us that b is also odd. We conclude that $\rho \equiv 1 + \sqrt{2} (\mathrm{mod}\, 2)$ in $O(\sqrt{2})$. Similarly $\nu \equiv 1 + \sqrt{2} (\mathrm{mod}\, 2)$.

By Lemma 8 there exist units $\lambda_1, \lambda_2 \in O(\sqrt{2})$ and quaternions $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{K}$ such that $\lambda_1\rho = N(\mathbf{q}_1)$ and $\lambda_2\nu = N(\mathbf{q}_2)$. Consider $\lambda_1\lambda_2\rho\nu = N(\mathbf{q}_1\mathbf{q}_2)$. Since $\lambda_1\lambda_2\rho\nu$ is the norm of an element of $\mathbb{K}$, it can be written as the sum of four squares of elements from $\mathbb{Q}(\sqrt{2})$ and is thus greater than zero. Taking conjugates with respect to $\mathbb{Q}(\sqrt{2})$ we find that $(\lambda_1\lambda_2\rho\nu)^*$ is also the sum of four squares of elements from $\mathbb{Q}(\sqrt{2})$ and is also greater than zero. Hence $\lambda_1\lambda_2\rho\nu$ is totally positive. Since ρ and ν are totally positive, we find that $\lambda_1\lambda_2$ is a totally positive unit of $O(\sqrt{2})$. This implies that $\lambda_1\lambda_2 = (1+\sqrt{2})^{2m}$ for some $m \in \mathbb{Z}$. A short computation shows that $N(\mathbf{q}_1\mathbf{q}_2)$ reduces to 1 modulo 2 in $O(\sqrt{2})$. Hence by Lemma 7 there exists a quaternion unit $\mathbf{u} \in \mathbb{K}$ of norm 1 such that $\mathbf{q}_1\mathbf{q}_2\mathbf{u} \in O(\sqrt{2})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$. Write $\mathbf{q}_1\mathbf{q}_2\mathbf{u}$ as $\alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ with α, β, γ

and δ in $O(\sqrt{2})$. Then

$$\lambda_1\lambda_2\rho v = N(\mathbf{q}_1\mathbf{q}_2) = N(\mathbf{q}_1\mathbf{q}_2\mathbf{u})$$
$$\Rightarrow (1+\sqrt{2})^{2m}\rho v = \alpha^2+\beta^2+\gamma^2+\delta^2. \tag{3.12}$$

Dividing both sides by the square unit $(1+\sqrt{2})^{2m}$ we find that ρv is the sum of four squares from the ring $O(\sqrt{2})$. $\square$

4. Cohn's theorem on sums of four squares

Theorem 11. *Every totally positive algebraic integer in $O(\sqrt{2})$ with even coefficient on the radical term is the sum of four squares from $O(\sqrt{2})$.*

Proof. Let $\alpha\in O(\sqrt{2})$ be as in the statement of the theorem. Then $\alpha = a+2b\sqrt{2}$. Taking this modulo 2 we find α is congruent to 0 or 1 modulo 2 in $O(\sqrt{2})$. By unique factorization we may write α as a unit times a product of primes, and with no loss of generality we may choose the primes to be totally positive. Thus

$$\alpha = \mu\cdot(2+\sqrt{2})^h\cdot p_1p_2\cdots p_k\cdot\gamma_1\gamma_2\cdots\gamma_m\cdot\beta_1\beta_2\cdots\beta_n, \tag{4.1}$$

where μ is a unit, $2+\sqrt{2} = \sqrt{2}(1+\sqrt{2})$ is a totally positive associate of $\sqrt{2}$, the p's are nonsplitting primes of $\mathbb{Z}$, the γ's are primes lying over rational primes congruent to 1 modulo 8, and the β's are primes lying over rational primes congruent to -1 modulo 8. We already know that the p's and the γ's can each be written as the sum of four squares from $O(\sqrt{2})$.

Since α and the primes in (4.1) are totally positive, μ must be totally positive also. Hence $\mu = (1+\sqrt{2})^{2t}$ for some $t\in\mathbb{Z}$. Taking (4.1) modulo 2

$$\alpha \equiv (3+2\sqrt{2})^t\cdot(2+\sqrt{2})^h\cdot p_1\cdots p_k\cdot\gamma_1\cdots\gamma_m\cdot\beta_1\cdots\beta_n(\text{mod }2),$$
$$\equiv \sqrt{2}^h(1+\sqrt{2})^n,$$
$$\equiv \{0 \text{ or } 1\} \pmod 2. \tag{4.2}$$

The congruences for the γ's and the β's were established in the proofs of the lemmas on representation by four squares in the previous section. There are three cases to consider, depending on the value of h.

If h is zero, then n must be even. Thus the β's can be paired up. The product of any pair of β's is the sum of four squares by Lemma 10. Since μ is a square, by the identity expressing the product of two sums of four squares as again a sum of four squares, we find that α can be written as a sum of four squares from $O(\sqrt{2})$.

If h is one and n is even then (4.2) reduces to the claim that 0 or 1 must be congruent to $\sqrt{2}\cdot 1$ modulo 2. If n is odd, (4.2) reduces to $\sqrt{2}(1+\sqrt{2}) \equiv \sqrt{2}(\mathrm{mod}2)$ being congruent to 0 or 1. In either case this is impossible.

If $h \geqslant 2$ then

$$\alpha = \mu \cdot 2(3+2\sqrt{2}) \cdot (2+\sqrt{2})^{h-2} \cdot p_1 \cdots p_k \cdot \gamma_1 \cdots \gamma_m \cdot \beta_1 \cdots \beta_n. \tag{4.3}$$

We previously showed that for each totally positive prime β lying over a rational prime congruent to -1 modulo 8 that there exists a unit $\lambda \in O(\sqrt{2})$ and a quaternion $\mathbf{q} \in \mathbb{K}$ such that $\lambda\beta = N(\mathbf{q})$. By the usual reasoning, λ is totally positive and thus must equal $(1+\sqrt{2})^{2d}$ for some $d \in \mathbb{Z}$. This gives $\beta = N((1+\sqrt{2})^{-d}\mathbf{q})$. Since $1+\sqrt{2}$ is a unit in $O(\sqrt{2})$ we find that β is the norm of some element of $\mathbb{K}$.

By the norm multiplication property there exists $\mathbf{r} \in \mathbb{K}$ for which $\beta_1\beta_2\cdots\beta_n = N(\mathbf{r})$. Also $(2+\sqrt{2})^{h-2} = N((\mathbf{w}_1+\mathbf{w}_2)^{h-2})$, and $\mu(3+2\sqrt{2}) = (1+\sqrt{2})^{2t+2}$. Thus

$$\mu \cdot (3+2\sqrt{2}) \cdot (2+\sqrt{2})^{h-2} \cdot \beta_1 \cdots \beta_n = N((1+\sqrt{2})^{t+1}(\mathbf{w}_1+\mathbf{w}_2)^{h-2}\mathbf{r}). \tag{4.4}$$

Let $\mathbf{s}$ be the expression inside the norm symbol of (4.4). It is clear that $\mathbf{s} \in \mathbb{K}$. By Lemma 6 there exists a quaternion unit $\mathbf{u} \in \mathbb{K}$ of norm 1 such that $\sqrt{2}\mathbf{su}$ is an element of $O(\sqrt{2})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$. Write $\sqrt{2}\mathbf{su}$ as $\theta_1 1 + \theta_2\mathbf{i} + \theta_3\mathbf{j} + \theta_4\mathbf{k}$ where $\theta_1, \ldots, \theta_4$ are elements of $O(\sqrt{2})$. Then

$$\begin{aligned} &\mu \cdot 2(3+2\sqrt{2}) \cdot (2+\sqrt{2})^{h-2} \cdot \beta_1 \cdots \beta_n \cdot 1 \\ &\quad = N(\sqrt{2} \cdot \mathbf{s} \cdot \mathbf{u}) \\ &\quad = \theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 \end{aligned} \tag{4.5}$$

is the sum of four squares of $O(\sqrt{2})$. Since $p_1 \cdots p_k \cdot \gamma_1 \cdots \gamma_m$ is the sum of four squares of $O(\sqrt{2})$, the product, α, is also the sum of four such squares. This proves the theorem of Cohn. □

5. The Icosians

A similar approach can be used to obtain an alternate proof of Götzky's four squares theorem for $\mathbb{Q}(\sqrt{5})$. Only an overview will be given as the demonstration is close in style to that of Cohn's four squares theorem. The corresponding ring is called the ring of icosians, denoted $\mathbb{I}$. We let $O(\sqrt{5})$ denote the integers in $\mathbb{Q}(\sqrt{5})$ and $\tau = (1+\sqrt{5})/2$ the fundamental unit. Then $\mathbb{I}$ can be thought of as the $O(\sqrt{5})$ module

with generators

$$\mathbf{e}_1 = \tfrac{1}{2}(1 + \tau^{-1}\mathbf{i} + \tau\mathbf{j}), \quad \mathbf{e}_2 = \tfrac{1}{2}(\tau^{-1}\mathbf{i} + \mathbf{j} + \tau\mathbf{k}),$$
$$\mathbf{e}_3 = \tfrac{1}{2}(\tau\mathbf{i} + \tau^{-1}\mathbf{j} + \mathbf{k}), \quad \mathbf{e}_4 = \tfrac{1}{2}(\mathbf{i} + \tau\mathbf{j} + \tau^{-1}\mathbf{k}) \tag{5.1}$$

as in Vignéras [11]. While there are 120 units of norm one in $\mathbb{I}$ we need only a small portion of these for our results.

Lemma 12. *The following are units in* $\mathbb{I}$ *of norm* 1.

$$\begin{aligned} &1, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \tau\mathbf{e}_3 - \mathbf{e}_2, \tau\mathbf{e}_4 - \mathbf{e}_3, \tau\mathbf{e}_2 - \mathbf{e}_4, \\ &-\mathbf{e}_1 + \tau^*\mathbf{e}_2 + \tau^*\mathbf{e}_3 + (1+\tau)\mathbf{e}_4, -\mathbf{e}_1 + \tau^*\mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4, \\ &-\mathbf{e}_1 - \tau\mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4, -\mathbf{e}_1 - \tau\mathbf{e}_2 + \mathbf{e}_3 + \tau\mathbf{e}_4, -\tau\mathbf{e}_1 - \mathbf{e}_2 + (1+\tau)\mathbf{e}_4, \\ &-\mathbf{e}_1 - \tau\mathbf{e}_2 + \tau\mathbf{e}_4, -\tau\mathbf{e}_1 - \mathbf{e}_2 + \tau\mathbf{e}_4. \end{aligned} \tag{5.2}$$

Lemma 13. $\mathbb{I} \cap \mathbb{R} = O(\sqrt{5})$.

Lemma 14. *For all* $\mathbf{a} \in \mathbb{I}$ *the quaternionic norm* $N(\mathbf{a}) \in O(\sqrt{5})$.

Lemma 15. *For all* $\mathbf{q} \in \mathbb{I}$ *there exist quaternion units* $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{I}$ *of norm* 1 *such that* $\mathbf{u}_1\mathbf{q}\mathbf{u}_2$ *has* $O(\sqrt{5})$*–integer coefficients, i.e.* $\mathbf{u}_1\mathbf{q}\mathbf{u}_2 \in O(\sqrt{5})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$.

Proof. *Let* $\mathbf{q} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \alpha_3\mathbf{e}_3 + \alpha_4\mathbf{e}_4$, where $\alpha_1, \ldots, \alpha_4 \in O(\sqrt{5})$. Write

$$\mathbf{q} = 2(\gamma_1\mathbf{e}_1 + \gamma_2\mathbf{e}_2 + \gamma_3\mathbf{e}_3 + \gamma_4\mathbf{e}_4) + (\delta_1\mathbf{e}_1 + \delta_2\mathbf{e}_2 + \delta_3\mathbf{e}_3 + \delta_4\mathbf{e}_4), \tag{5.3}$$

where $\gamma_1, \ldots, \gamma_4 \in O(\sqrt{5})$ and $\delta_1, \ldots, \delta_4 \in O(\sqrt{5})/(2)$. Note that a full set of residues of $O(\sqrt{5})$ modulo 2 can be chosen as $\{0, 1, \tau, \tau^*\}$. Computation shows that for all possible values of $\delta_1, \ldots, \delta_4$ there exists quaternion units $\mathbf{u}_1, \mathbf{u}_2$ in (5.2) such that $\mathbf{u}_1(\delta_1\mathbf{e}_1 + \cdots + \delta_4\mathbf{e}_4)\mathbf{u}_2$ is an element of $O(\sqrt{5})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$. The proof continues in an analogous fashion to Lemma 6. □

Lemma 16. *Suppose* ρ *is a prime of the ring* $O(\sqrt{5})$. *Then there exists a unit* λ *of* $O(\sqrt{5})$ *and a quaternion* $\mathbf{q}$ of $\mathbb{I}$ *such that* $N(\mathbf{q}) = \lambda\rho$.

Proof. The proof is completely analogous to that of Lemma 8. One small difference is in the case where ρ lies over the rational prime p which splits. In this case, by geometry of numbers there exists α, β, γ and δ in $O(\sqrt{5})$ such that $\alpha^2 + \beta^2 + \gamma^2 +$

$\delta^2 = \kappa\rho$ with $|\kappa\kappa^*| \leqslant 8$ and $\kappa \in O(\sqrt{5})$. The proof then continues in the same fashion as in Lemma 8. □

Lemma 17. *Let ρ be a totally positive prime of the ring $O(\sqrt{5})$ lying over the rational prime p. Then ρ can be written as the sum of four squares of algebraic integers from $O(\sqrt{5})$.*

Proof. By Lemma 16 there exists a quaternion $\mathbf{q} \in \mathbb{I}$ and a unit $\lambda \in O(\sqrt{5})$ such that $N(\mathbf{q}) = \lambda\rho$. We may write $\mathbf{q}$ as $\alpha 1 + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$, where α, β, γ and δ are in $\mathbb{Q}(\sqrt{5})$. Thus

$$\lambda\rho = N(\mathbf{q}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0. \tag{5.4}$$

Taking conjugates with respect to $\mathbb{Q}(\sqrt{5})$ we find $\lambda^*\rho^*$ is also a sum of squares and greater than zero. Thus $\lambda\rho$ is totally positive from which it follows that λ itself is totally positive. Note that $\lambda = \pm\tau^n$ for some rational integer n. Together this implies that $\lambda = \tau^n$ and n is even. We can therefore write $N(\mathbf{q}) = \tau^{2m}\rho$ for some $m \in \mathbb{Z}$.

By Lemma 15 there exist quaternion units of norm one, $\mathbf{u}_1, \mathbf{u}_2$, such that $\mathbf{u}_1\mathbf{q}\mathbf{u}_2 \in O(\sqrt{5})[1, \mathbf{i}, \mathbf{j}, \mathbf{k}]$. Write

$$\mathbf{u}_1\mathbf{q}\mathbf{u}_2 = \hat{\alpha}\,1 + \hat{\beta}\,\mathbf{i} + \hat{\gamma}\,\mathbf{j} + \hat{\delta}\,\mathbf{k}, \quad \hat{\alpha}, \hat{\beta}, \hat{\gamma}, \hat{\delta}, \in O(\sqrt{5}). \tag{5.5}$$

Then

$$\tau^{2m}\rho = N(\mathbf{q}) = N(\mathbf{u}_1\mathbf{q}\mathbf{u}_2) = (\hat{\alpha})^2 + (\hat{\beta})^2 + (\hat{\gamma})^2 + (\hat{\delta})^2. \tag{5.6}$$

Dividing by τ^{2m} gives the desired representation of ρ. □

Theorem 18. *Every totally positive algebraic integer in $O(\sqrt{5})$* is the sum of four squares from $O(\sqrt{5})$.

Proof. This follows as in Deutsch [5]. □

6. Further directions

It appears plausible that the technique of combining geometry of numbers bounds with special rings of quaternions can lead to more results of similar type. Due to a result of Siegel [10] sums of squares are not universal for any totally real number fields besides the rational integers and the integers in $\mathbb{Q}(\sqrt{5})$. Restricting to cases analogous to Cohn's four squares theorem does not improve matters. Assuming the discriminant of the quadratic field is divisible by four and totally positive integers under consideration have even irrational coefficients, numerical computations imply

that only in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are the sum of four squares universal for this limited class of integers.

It would be interesting to formulate a condition in general number fields which insures that a totally positive integer satisfying such condition is the sum of four integer squares. Such general results would most likely require much deeper techniques than those used in this paper.

7. The computation

The computations utilized the PUNIMAX variant of MAXIMA on a Pentium 133 chip personal computer with 32 megabytes of RAM. The operating system was LINUX 2.0.35. The running time to perform the computations relevant to Lemmas 6 and 7 totaled 8 min and 24 s. Two SNOBOL4 programs were written to transform the MAXIMA output into TEX readable form for Tables 1 and 2. The computation for Lemma 15 required 85.58 min. A table for the products of pairs of basis elements $\mathbf{w_1}, \ldots, \mathbf{w_4}$ was created. Using this, the entries appearing in Tables 1 and 2 were checked by manual calculation.

Acknowledgments

The author express his appreciation to the Mathematics Department of the University of Botswana for the use of their facilities. The author thanks B. Haible, the maintainer of PUNIMAX, for permitting its free use for academic purposes [7], Prof. Vignéras for clarifying an essential point about the cubians, and Michael Rosen for raising the issue of representations in general number fields. He also thanks Don Hadwin and Jiankui Li for helping him find the paper of Siegel [10], and Harvey Cohn for many encouraging E-mail communications.

References

[1] M. Baake, R. Moody, Similarity submodules and root systems in four dimensions, Canad. J. Math. 51 (1999) 1258–1276.
[2] H. Cohn, Decomposition into four integral squares in the fields $2^{1/2}$ and $3^{1/2}$, Amer. J. Math. 82 (1960) 301–322.
[3] H. Cohn, Calculation of class numbers by decomposition into three integral squares in the fields of $2^{1/2}$ and $3^{1/2}$, Amer. J. Math. 83 (1961) 33–56.
[4] H. Cohn, Cusp forms arising from hilbert's modular functions for the field of $3^{1/2}$, Amer. J. Math. 84 (1962) 283–305.
[5] J.I. Deutsch, Geometry of numbers proof of Götzky's four squares theorem, J. Number Theory 96 (2) (2002) 417–431.
[6] F. Götzky, Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher, Math. Ann. 100 (1928) 411–437.
[7] B. Haible, Private communication, 1997.

[8] G. Hardy, E. Wright, An Introduction to the Theory of Numbers, 4th Edition, Oxford University Press, London, 1971.
[9] Herstein, Topics in Algebra, J Wiley, New York, 1975.
[10] C.L. Siegel, Sums of mth Powers of Algebraic Integers, Ann. Math. 46 (2) (1945) 313–339.
[11] M.-F. Vignéras, Arithmétique des Algèbres de Quaternions, Lecture Notes in Mathematics, Vol. 800, Springer, New York, 1980.